AKAMAI CHECKLIST

Zero Trust Platform Capabilities

An effective Zero Trust platform consolidates once-distinct point solutions — including Zero Trust Network Access (ZTNA), microsegmentation, DNS firewall, and threat hunting — into an integrated, single-console platform. Quick and effective deployment of Zero Trust means stopping ransomware, meeting demanding compliance mandates, and securing your distributed workforce as well as your hybrid cloud infrastructure. This checklist can be used to assess vendor capabilities, or as a list of requirements to implement Zero Trust with a single platform.

Category 1: Platform requirements

Your Zero Trust platform solution should be flexible, scalable, and easy to administer.

□ Scalability to match traffic demands and provide continuous protection without loss of performance

□ Ability to integrate with existing security tools that customers currently have in place, such as SIEM, SOAR, EDR, CMDB, and more

□ Coverage for heterogeneous data centers — hybrid and multicloud environments, legacy systems, end-user devices, Kubernetes clusters, virtual machines, IoT/OT environments, and more

□ Flexible deployment models supporting diverse hybrid architectures — cloud, virtual, on-premises

□ Ability to accommodate both agent-based and agentless deployments (IoT/OT, PaaS)

□ Support for Windows, Linux, and macOS, as well as legacy operating systems

□ Audit log capabilities to ensure the recording of all actions

Akamai

Category 2: Visibility requirements

Deep visibility is critical to understanding the environment, identifying suspicious connections, and responding quickly and precisely to threats.

- □ Map-like visualization of all applications and workload flows as well as user-to-application access across any environment — containers, serverless, IaaS or PaaS — all from a single console
- □ Historic and real-time flows for investigation and forensics
- □ Interoperability with third-party firewalls and hardware such as switch devices
- □ Ability to collect data from various third-party sources such as CMDB, EDR, and cloud APIs for contextual labels and rules
- □ Labeling assistance, preferably leveraging AI for speed and accuracy

Category 3: Policy requirements

Both east-west (microsegmentation) and north-south (ZTNA) policies are applied from one place, based on attributes that can be used in a range of use cases such as ransomware protection, remote workforce protection, zero-day response, and compliance.

- □ Policy that is software-defined and distributed throughout the enterprise without requiring physical internal firewalls that create chokepoints
- □ Rules created based on various workload attributes rather than only IPs and ports
- □ Granular application-centric policies enforced so workloads are protected down to the port, process, and even service level
- □ A policy recommendation engine with out-of-the-box and custom templates, preferably leveraging AI, that accelerates policy creation
- □ Policies enforced with or without an agent
- □ Policy controls based on comprehensive flow mapping
- □ Preconfigured policies for global risk reduction based on industry best practices
- □ Policy for hybrid cloud across virtualized, IaaS, and PaaS environments
- □ Policies tied to the workload with the ability to follow it if it moves, migrates, or changes
- □ Access policy for users in the office and working remotely

Category 4: Zero Trust component requirements

Of the various functions integrated into a unified Zero Trust platform, Zero Trust Network Access and microsegmentation stand out as the foundational pillars. These technologies enable organizations to deploy Zero Trust controls without negatively impacting the workforce and business continuity.

- □ Unified access and network policy engine (combined east-west and north-south control)
- □ Strong identity enforcement with FIDO2 multi-factor authentication (MFA)
- □ Ability to protect IT environments and users from a broad range of threats by monitoring and filtering DNS traffic
- □ Ongoing detection of evasive threats and monitoring of security posture
- □ Signal sharing across the platform tools to ensure an attacker is stopped even if they manage to punch through the access mechanism
- □ Adoption of dynamic deception systems capable
of tracking and quarantining attackers
- □ Ability to query endpoints or servers for the presence of vulnerabilities to allow quick ransomware detection mitigation

Category 5: Integrated AI requirements

Many aspects of effectively implementing Zero Trust can be streamlined with the use of AI. This expedites and simplifies policy creation, compliance, incident response, and vulnerability assessment.

- □ Communication with network logs using natural language to help shorten the time to incident response, compliance scoping efforts, and more
- □ Streamlining of the entire policy process with AI that suggests labels and policies based on your unique traffic patterns
- □ Translation of natural language into syntax to quickly look for vulnerabilities in your network without having to research IOCs or write custom queries
- □ AI threat hunting mechanisms for advanced detection methods to find anomalies and malicious activity that traditional tools miss

Please visit Akamai Zero Trust Security to learn more.

| Support | | Published 04/24